IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

IN RE: DEALER MANAGEMENT SYSTEMS ANTITRUST LITIGATION This Document Relates To: *Authenticom, Inc. v. CDK Global, LLC, et al.*, Case No. 1:18-cv-00868 (N.D. Ill.)	MDL No. 2817 Case No. 18-cv-00864 Hon. Robert M. Dow, Jr. Magistrate Judge Jeffrey T. Gilbert **PUBLIC-REDACTED**

PLAINTIFF AUTHENTICOM, INC.'S RESPONSES TO COUNTERCLAIMANT'S THE REYNOLDS AND REYNOLDS COMPANY'S STATEMENT OF UNDISPUTED MATERIAL FACTS IN SUPPORT OF ITS MOTION FOR PARTIAL SUMMARY JUDGMENT

GLOSSARY

Abbreviation	Full Citation
ACOM SUF	Authenticom, Inc.'s Statement of Undisputed Material Facts in Support of Its Motion for Summary Judgment on Defendants' Counterclaims (Dkt. 977)
PJ SAF	MDL Plaintiffs' Statement of Additional Facts in Opposition to Defendants' Motion for Summary Judgment
Dorris Ex.	Exhibits to the Declaration of Daniel V. Dorris in Support of Plaintiff Authenticom, Inc.'s Motion for Summary Judgment on Defendants' Counterclaims (Dkt. 977-1)
Emmanual Ex.	Exhibits to the Declaration of Jonathan Emmanual in Support of The Reynolds and Reynolds Company's Motion for Partial Summary Judgment (Dkt. 779-2)
Fenske Ex.	Exhibits to the Declaration of Daniel Fenske in Support of Defendants CDK Global, LLC's And The Reynolds And Reynolds Company's Motion For Summary Judgment (Dkt. 975)
Ho Ex.	Exhibits to the Declaration of Derek T. Ho in Support of MDL Plaintiffs' Oppositions to Defendants' Motions for Summary Judgment
Wilkinson Ex.	Exhibits to the Declaration of Brice Wilkinson in Support of Reynolds's Motion for Partial Summary Judgment (Dkt. 779-1)

Plaintiff Authenticom, Inc. ("Authenticom") responds as follows to The Reynolds and Reynolds Company's ("Reynolds") Statement of Undisputed Material Facts in Support of Its Motion for Summary Judgment (Dkt. 779). Authenticom objects that Reynolds's Statement of Undisputed Material Facts includes narrative paragraphs asserting multiple facts, contrary to Local Rule 56.1(a)(3) which requires that "the numbered paragraphs be short; they should contain only one or two individual allegations, thereby allowing easy response. . . . [I]t is inappropriate to confuse the issues by alleging multiple facts in a single paragraph in hopes of one's opponent missing one." *Malec v. Sanford*, 191 F.R.D. 581, 583 (N.D. Ill. 2000); *see Civix-DDI, LLC v. Cellco P'ship*, 387 F. Supp. 2d 869, 881 (N.D. Ill. 2005) (rule violated by "lengthy paragraphs purporting to be individual facts"). Further, Authenticom objects that many statements of fact improperly make legal argument. *See Judson Atkinson Candies, Inc. v. Latini-Hohberger Dhimantec*, 529 F.3d 371, 382 n.2 (7th Cir. 2008) ("It is inappropriate to make legal arguments in a Rule 56.1 statement of facts."). Finally, Authenticom objects to the extent that Reynolds has not cited material to support the asserted fact. *See* Local Rule 56.1(a) (requiring "specific references to the affidavits, parts of the record, and other supporting materials relied upon to support the facts set forth in that paragraph"); *Prince v. Stewart*, 2011 WL 1193205, at *1 (N.D. Ill. Mar. 30, 2011) ("Because defendants have offered no evidentiary basis for the 'facts' asserted in these paragraphs, they are inadmissible speculation."); *Barth v. Village of Mokena*, 2006 WL 862673, at *3 (N.D. Ill. Mar. 31, 2006) (striking facts where "material relied upon . . . did not support the facts . . . asserted").

By stating that a fact is undisputed, Authenticom does not dispute the fact solely in connection with Reynolds's motion for summary judgment on its counterclaims (Dkt. 777). Further by stating that a fact is undisputed, Authenticom does not concede the admissibility or sufficiency of any specific evidence, the materiality of any fact asserted, or the legal significance

of any fact or evidence. This response corresponds with the paragraph numbering used in Reynolds's Statement of Undisputed Material Facts. Authenticom does not respond to Reynolds's headings or footnotes which do not purport to constitute statements of facts.

AUTHENTICOM'S RESPONSES

1. Reynolds owns, develops, and supports the Reynolds Dealer Management System ("DMS"). The Reynolds DMS is an enterprise computer software platform licensed by automotive dealerships to manage their business. Reynolds provides two DMS platforms, called ERA and POWER. ERA also has an enhanced user-interface version known as "ERA-IGNITE." Declaration of R. Schaefer [Auth. Dkt. 97] ¶¶ 1, 6-7, 9, 14; Declaration of R. Lamb [Auth. Dkt. 98] ¶¶ 2, 4, 5-6; Ex. 1 at 34:3-16, 94:3-25 (Burnett tr.) (discussing ERA and ERA-Ignite); Ex. 2 at 63:22-64:2 (Kirby tr.).

RESPONSE: Undisputed.

2. The Reynolds DMS is comprised of multiple hardware and software components. The Reynolds DMS's "core" functionalities manage a dealer's accounting, parts, service, inventory, and sales operations. Declaration of R. Schaefer [Auth. Dkt. 97] ¶¶ 2, 4; Declaration of R. Lamb [Auth. Dkt. 98] ¶¶ 2, 5.

RESPONSE: Undisputed.

3. Reynolds licenses its proprietary DMS to automotive dealerships pursuant to a license contract. That agreement expressly limits the scope of the Reynolds DMS license solely to dealership employees who have a need for access to operate the dealership's business. The agreement does not allow dealers to sublicense the Reynolds DMS, grant access to or share the DMS with any third parties, or connect any third-party software to the Reynolds DMS without

Reynolds's express written permission. These restrictions are plain on the contracts' face, are well known in the automotive industry, and have been in place for more than 12 years. Declaration of R. Schaefer [Auth. Dkt. 97] ¶¶ 14, 17, 18; Declaration of R. Lamb [Auth. Dkt. 98] ¶ 3, 20-21; Ex. at 314:3-11 (Brockman tr.); Ex. 4, REYMDL00677044 § 1 (Reynolds Master Agreement) [redacted]; Ex. 5, REYMDL00012246 (Reynolds Customer Guide), at 256 [redacted] at 265 [redacted] at 267 [redacted] Ex. 6, REYMDL00675678 (Reynolds Defined Terms list); Ex. 92, REYMDL01075468 § 15.2.3 (Penske 2018 Agreement); Ex. 94, REYMDL00676893 (Reynolds Authorization Letter).

RESPONSE: Undisputed that Reynolds licenses its DMS pursuant to a license contract. Disputed that the licenses impose the restrictions asserted by Reynolds. As an initial matter, these are legal conclusions, to which no response is required. Further, Reynolds's legal argument is contrary to the plain terms of the license agreement, which provides that [redacted]

[redacted]. Emmanual Ex. 6 [Dkt. 779-8] at -679; Emmanual Ex. 4 [Dkt. 779-6] at -044.

4. The Reynolds DMS license's restrictions on third-party access were also the subject of a 2012 lawsuit between Reynolds and a third-party data broker called Superior Integrated Solutions ("SIS"), which resulted in a federal court decision holding that Reynolds's DMS contracts forbid third-party access. Ex. 7, REYMDL00015586 ¶¶ 49-57 (Reynolds v. SIS Complaint); *Reynolds & Reynolds Co. v. Superior Integrated Sols., Inc.*, 1:12-CV-848, 2013 WL 2456093, at *2 (S.D. Ohio June 6, 2013). [redacted]. Ex. 8, REYMDL00022780 (Reynolds-SIS Settlement Agreement).

RESPONSE: Objected to and disputed in part. Undisputed that there was a 2012 lawsuit between Reynolds and SIS in which Reynolds alleged that SIS's access was unauthorized, and that the lawsuit resulted in a settlement that required SIS to cease accessing Reynolds's DMS after a certain period of time. Objected to in that the lawsuit and the settlement are not admissible evidence against Authenticom. *See* Fed. R. Civ. P. 56(c)(2). Disputed that SIS is a "data broker." Reynolds cites no facts to support that characterization. Further disputed that there was a "holding that Reynolds's DMS contracts forbid third-party access." This is a legal conclusion to which no response is required. Further, the Court merely took judicial notice of certain provisions in Reynolds's contracts, without addressing the relevant provisions that dealers' [redacted] *See Reynolds & Reynolds Co. v. Superior Integrated Sols., Inc.*, 2013 WL 2456093, at *2 (S.D. Ohio June 6, 2013). In any event, the Court's rulings are not binding on Authenticom, which was not a party to Reynolds's lawsuit against SIS.

Disputed that SIS's access was "hostile" as opposed to approved by a dealer. *See* Ho Ex. 30, Battista Tr. 31:23-32:18.

5. When a user accesses the Reynolds ERA DMS, they do so via a program called ERAccess.exe or ERA-Ignite.exe. Both programs are Reynolds's registered copyrighted intellectual property. Ex. 9 (Copyright TX 7-586-896); Ex. 10 (Copyright TX 7-586-863); Ex. 11 (Copyright TX 8-538-825); Ex. 12 (Copyright TX 8-538-541). A user must first enter a valid set of credentials (user ID and password). After entering those credentials, they are then able to access the rest of the ERA system, which is also Reynolds's copyrighted (although not registered) intellectual property. *See* Auth. P.I. Tr. 2-P [Auth. Dkt. 163] at 14 (Testimony of R. Schaefer); Declaration of R. Schaefer [Auth. Dkt. 97] ¶¶ 4, 14, 27; Ex. 13 (Login screen for ERAccess, version 27.250); Ex. 14, REYMDL00022920 (Aug. 19, 2010 ERAccess announcement); Ex. 15, REYMDL00022918 (Jan. 14, 2011 ERAccess announcement).

RESPONSE: Undisputed that users access Reynolds's DMS through ERAccess.exe and ERA-Ignite.exe and that Reynolds has registered copyrights in those executable programs. Undisputed that a user must enter credentials to use those programs. The remaining assertions regarding whether the executable programs or "the rest of the ERA system" are intellectual property or are subject to copyright protection are legal conclusions to which no response is required. Reynolds also does not present facts to support those legal conclusions. To the extent that they can be considered factual assertions, they are disputed. For example, at least portions of "the rest of the ERA system" are not subject to copyright protection. *See* Dorris Ex. 155 [Dkt. 977-157] Miracle Rebuttal Rep. ¶¶ 110-12.

6. Reynolds has developed software tools that allow dealership employees to export dealers' operational data from the Reynolds DMS. The current version of this tool is called Dynamic Reporting. Dynamic Reporting allows dealer employees to create custom reports with their specified data fields and formats. Reports can be saved, and any report can be scheduled to run automatically up to four times a day. Declaration of R. Schaefer [Auth. Dkt. 97] ¶ 86; Ex. 23 at 42:19-44:6 (Reynolds 30(b)(6) Hall tr.).

RESPONSE: Undisputed.

7. Once a dealership employee has exported a dealership's operational data from the Reynolds DMS, Reynolds places no contractual or technological restrictions on the dealership's use of that data. Declaration of R. Schaefer [Auth. Dkt. 97] ¶ 87.

RESPONSE: Undisputed.

8. Some dealers choose to send or transmit data that they exported from the Reynolds DMS using Dynamic Reporting to Authenticom. Declaration of R. Schaefer [Auth. Dkt. 97] ¶ 87; Ex. 24 at 70:10-19 (Wiersgalla tr.); Ex. 44 at 141:12-142:21 (Hembd tr.); Ex. 96, AUTH_00150633.

RESPONSE: Undisputed.

9. In addition, Reynolds offers its dealership customers the option of having Reynolds automatically transfer the dealerships' vehicle inventory data (data that does not contain any sensitive personally identifiable information) to an FTP site through Reynolds's AVID (Automated Vehicle Inventory Data) product. Once the data is moved outside of the DMS,

Reynolds places no contractual or technical restrictions on the dealership's ability to provide access to this data, including to Authenticom. Declaration of R. Schaefer [Auth. Dkt. 97] ¶ 90; Ex. 39 at 188:8-189:14 (Munns tr.); Ex. 95, AUTH_00067483.

RESPONSE: Undisputed.

10. Reynolds merged with another DMS provider, Dealer Computer Services, in 2006. Dealer Computer Systems owned the POWER DMS product, while Reynolds owned the ERA DMS product. At that time, POWER was a secure, stable DMS platform that enjoyed the benefit of that reputation in the marketplace. ERA, in contrast, had serious security holes. For example, the ERA DMS was still using dial-up modems for communications. After the merger, Reynolds worked to improve ERA's security. Ex. 3 at 15:1-16:23; 303:9-304:11 (Brockman tr.); Declaration of R. Schaefer [Auth. Dkt. 97] ¶¶ 7, 9, 28-30; Ex. 16 at 31:24-33:9 (Lamb tr.).

RESPONSE: Disputed that POWER DMS was a "secure, stable" product with a positive market reputation. POWER DMS has a small market share. *See* Ho Ex. 61, Bresnahan Rep. ¶ 45. Disputed to the extent Reynolds's statement addresses the reasons for its blocking of data integrators from its DMS. *See also* Responses to Statement of Fact Nos. 11-12.

11. A core part of Reynolds's security strategy was to eliminate the security holes that were being exploited by third parties to hostilely access to the Reynolds DMS. Mr. Brockman and others at Reynolds regularly announced this policy and strategy to the automotive industry and industry publications widely reported it. Ex. 3 at 304:12-25 (Brockman tr.); Ex. 17 (January 2007 Automotive News Article); Ex. 107, REYMDL00012341 (February 2007 Automotive News Article) ("Reynolds, with about 11,000 dealership customers in the United States, has warned

dealers that they are violating their contracts when they provide log-ins and passwords to third-party vendors."); Ex. 18, REYMDL00022899 (Fuel Article January 1, 2010: "It remains our policy to not allow 'hostile interfaces' or unauthorized code on your systems to protect both Reynolds and your dealership from security breaches and potential data corruption issues."); Ex. 108 (same Fuel article, submitted by Authenticom as preliminary injunction exhibit 14 [Auth. Dkt. 64-14]; Ex. 19 (AUTH_00170940) (Authenticom 2013 announcement that Reynolds was "steadfast in their commitment to remove all 3rd party access points to their system").

RESPONSE: Undisputed that Reynolds announced a "policy and strategy" of preventing access by "third parties" (but not agents). Disputed that Reynolds had effectuated this "policy and strategy" until approximately 2017. Reynolds made numerous "whitelisting" exceptions, including allowing more than [redacted] User IDs to be used by data integrators as of March 2015. *See* ACOM SUF 69-70; PJ SAF 27-28; *see also* Wilkinson Ex. 83 [Dkt. 78-34] (November 15, 2013: Authenticom employee joking about how Reynolds had "been saying they were going to lock everyone out" for eight years without following through). Reynolds's exceptions were driven by dealer dissatisfaction with Reynolds's "policy and strategy" and competition from CDK. *See* PJ SAF 24-26.

Disputed that prohibiting "third-party" access was a "security strategy." Reynolds's efforts to inhibit third-party access were, at least in part, driven by the profit motive of transitioning application vendors to Reynolds's Certified Interface ("RCI"). *See* Ho Ex. 22, Whitworth Tr. 299:7-300:1 [redacted]

[redacted] Dorris Ex. 93, at -887 [redacted] Ho Ex. 119 at -263 [redacted]

Disputed that "third parties" were "exploiting" any "security holes" to "hostilely access" the DMS. Data integrators were dealers' properly authorized agents, using the DMS in the same manner as a dealer employee. *See* Dorris Ex. 5 [Dkt. 977-6] ¶ 24 ("Before Authenticom pulls data from a dealership, it gets specific authorization from the dealer."); *id.* ¶ 25 ("Once dealers set up login credentials for Authenticom, Authenticom automates the pulling of data through user emulation software, which uses the DMS application software to run and capture reports in the same way a user at a dealership would. The difference is that integrators like Authenticom automate the process, whereas a user at the dealership would retrieve the data manually."); *see* Response to Statement of Fact No. 3.

12. Reynolds took early steps to better secure and control access to its ERA DMS. These steps included:

- Requiring all dealership employees to use a unique set of login credentials (including a user ID and password) to access the DMS;
- Removing all third-party software from Reynolds DMS servers;
- Ending modem access to the Reynolds DMS;
- Requiring regular DMS password changes; and
- Requiring Reynolds DMS users to use only Reynolds's approved terminal software to access the DMS.

Declaration of R. Schaefer [Auth. Dkt. 97] ¶¶ 29-30; Ex. 20, REYMDL00015519 (2016 ERA Data

Management Milestones); Ex. 21, REYMDL00015521 (2011 ERA Data Management Milestones).

RESPONSE: Undisputed that Reynolds took these steps at some point in time. To the extent Reynolds claims these steps improved the security of Reynolds's DMS, Reynolds has not presented any evidence in support of that assertion. Also disputed that Reynolds took these normal security steps "early," which is vague and unsupported by any cited evidence.

13. Reynolds continued to implement access control measures over time. For example, Reynolds implemented CAPTCHA prompts and challenge questions, which require users to answer questions intended to prove they are human dealership employees. CAPTCHA prompts are a form of Turing test; their purpose is to prevent automated processes or machines from assessing a computer system. Ex. 16 at 64:23-65:6 (Lamb tr.); Ex. 22 at 68:4-9 (Hill tr.); Ex. 23 at 48:7-18 (Reynolds 30(b)(6), Hall tr.); Declaration of R. Schaefer [Auth. Dkt. 97] ¶ 30; Ex. 24 at 86:4-24 (Wiersgalla tr.); Ex. 25 at 337:23-338:22 (SIS 30(b)(6), Battista tr.).

RESPONSE: Undisputed that Reynolds has implemented CAPTCHA prompts and challenge questions at some point in time. However, disputed to the extent Reynolds's statement suggests that it consistently used these measures after their introduction. *See* Response to Statement of Fact No. 11 (explaining that Reynolds's blocking measures were subject to numerous exceptions and constrained by competition by CDK prior to September 2013). Reynolds's assertions as to the "purpose" of CAPTCHA prompts and challenge questions are vague as to whose purpose is being described, and also disputed to the extent they suggest that such measures are meant to prevent automated data polling. *See* Ho Ex. 58, Miracle Tr. 33:21-37:21. Indeed, there is no prohibition in Reynolds's contracts with dealers against use of automated data polling

by dealers or their agents. *See* Emmanual Ex. 5 [Dkt. 779-7] at -265 [redacted] Emmanual Ex. 6 [Dkt. 779-8], at -679 [redacted] (emphasis added). Further disputed to the extent that Reynolds asserts CAPTCHA or challenge questions are access controls within the meaning of the Digital Millennium Copyright Act. *See* 17 U.S.C. § 1201(a)(3)(B). This is a legal conclusion to which no response is required.

14. Reynolds first introduced its "Challenge Questions" (e.g., "What color is the sky?") in 2009. Reynolds then introduced ASCII CAPTCHAs in 2010, and later replaced those with graphical CAPTCHAs starting in 2012. Ex. 20, REYMDL00015519 (2016 ERA Data Management Milestones); Ex. 26, AUTH_00468320 (Authenticom timeline chart including introduction of CAPTCHA and challenge questions); Ex. 27, REYMDL00101073 at 23 (showing CAPTCHA security check prompt); Ex. 28 at 46:14-17, 48:13-24 (Clements tr.) (describing Reynolds challenge questions and ASCII CAPTCHAs); Ex. 16 at 65:7-17 (Lamb tr.) (describing Reynolds's long history of CAPTCHA use); Declaration of S. Cottrell [Auth. Dkt. 51] ¶ 37 ("Reynolds first started disabling Authenticom's polling services in 2009 when it introduced "challenge questions" and 'captcha' (where the user has to enter random blurred text) to make it more difficult to automate the pulling of data."); Ex. 29 at 172:7-11 (Cottrell 2019 tr.) ("Reynolds was using CAPTCHA as part of their log-on process, you know, under DMS."); Authenticom Resp. to Defs. Statement of Add'l Facts [Auth. Dkt. 145] (hereinafter "Auth. Resp. to DSAF")

¶¶ 75, 76 ("Undisputed that Reynolds implemented a series of roadblocks to prevent dealers from using independent integrators, including challenge questions and captcha.").

RESPONSE: Undisputed to the extent "introduced" means "began to use." However, disputed to the extent Reynolds's statement suggests that it consistently used these measures after their introduction. *See* Response to Statement of Fact No. 11 (explaining that Reynolds's blocking measures were subject to numerous exceptions and constrained by competition by CDK prior to September 2013).

15. Reynolds also developed a "Suspicious User ID" detection system, which detected patterns and actions that were inconsistent with a normal dealership employee's use of the system and disable the associated ID. Auth. P.I. Tr. 2-P [Auth. Dkt. 163] at 15, 16 (Testimony of R. Schaefer); Ex. 30, REYMDL00001971, at 1976-1977 (ERA May 2013 Release Notes).

RESPONSE: Disputed in part. Disputed to the extent Reynolds's statement suggests that it consistently used these measures after their introduction. *See* Response to Statement of Fact No. 11 (explaining that Reynolds's blocking measures were subject to numerous exceptions and constrained by competition by CDK prior to September 2013). Disputed that Suspicious User ID monitoring would immediately disable a user ID; the user ID would be "flagged," and the user ID would display an error message at the next login attempt. *See* Emmanual Ex. 31 [Dkt. 779-33] [redacted] Emmanual Ex. 30 [Dkt. 779-32] at -977 [redacted]

16. On August 8, 2011, Reynolds announced the rollout of this security enhancement that monitored, detected, and disabled user IDs using automated access methods. Ex. 31, REYMDL00022904 (August 8, 2011 Reynolds System Announcement); Declaration of S. Cottrell [Auth. Dkt. 51] ¶ 37.

RESPONSE: Disputed that these were "security" enhancements. Reynolds's efforts to inhibit third-party access were, at least in part, driven by the profit motive of transitioning application vendors to RCI. *See* Response to Statement of Fact No. 11. Disputed that Suspicious User ID monitoring would immediately disable a user ID; the user ID would be "flagged," and the user ID would display an error message at the next login attempt. *See* Emmanual Ex. 31 [Dkt. 779-33] [redacted] Emmanual Ex. 30 [Dkt. 779-32] at -977 [redacted]

17. In May 2013, Reynolds released the enhanced version of this monitoring system, known as the Suspicious User ID process, for its ERA DMS. As described in the user guide for this release, the process was used to track and prevent suspicious system activity. Any user ID attempting to access the system with software or a communications method not supported by Reynolds—i.e., any hostile or automated method—would be immediately disabled. *See* Ex. 30, REYMDL00001971, at 1976-1977; Auth. Resp. to DSAF [Auth. Dkt. 145] ¶ 77; Declaration of R. Schaefer [Auth. Dkt. 97] ¶ 30; Ex. 32, AUTH_00219452 (containing examples of disabled Authenticom IDs and associated screenshots from the Reynolds DMS); Declaration of S. Cottrell

[Auth. Dkt. 51] ¶ 38 (testifying that Reynolds disabled 27,000 profiles used by Authenticom in summer 2013).

RESPONSE: Disputed that Reynolds's intent was to "track and prevent suspicious system activity." Reynolds's efforts to inhibit third-party access were, at least in part, driven by the profit motive of transitioning application vendors to RCI. *See* Response to Statement of Fact No. 11. Reynolds sought to impede legitimate dealer-authorized access. *See* Response to Statement of Fact No. 3. Undisputed that Reynolds referred to this access as "hostile or automated." Disputed that Suspicious User ID monitoring would immediately disable a user ID; the user ID would be "flagged," and the user ID would display an error message at the next login attempt. *See* Emmanual Ex. 31 [Dkt. 779-33] [redacted] Emmanual Ex. 30 [Dkt. 779-32] at -977 [redacted]

18. Reynolds's monitoring process looks for indicia of automated (non-human) use. That includes patterns of activity (e.g., only running data reports), timing of activity (e.g., only accessing the system in the middle of the night), timing of inputs (e.g., typing faster than a human can), and patterns of inputs (e.g., use of a virtual rather than physical keyboard to send input commands). As part of its Suspicious User ID measure, the Reynolds system disallowed or disabled IDs that used [redacted]. If a user ID fails the Reynolds criteria, the ID is deemed suspicious and its access to the Reynolds DMS is disabled. Auth. P.I. Tr. 2-P [Auth. Dkt. 163] at 15, 16 (Testimony of R. Schaefer); Ex. 33, AUTH_00141204; Ex. 34,

AUTH_00093108; Ex. 35, AUTH_00141219; Ex. 36, AUTH_00167914; Ex. 32, AUTH_00219452.

RESPONSE: Disputed in part. Disputed that Suspicious User ID monitoring would immediately disable a user ID; the user ID would be "flagged," and the user ID would display an error message at the next login attempt. *See* Emmanual Ex. 31 [Dkt. 779-33] [redacted] Emmanual Ex. 30 [Dkt. 779-32] at -977 [redacted]

19. These access-control measures were targeted at a variety of potential threats, including (a) any attempts to access the Reynolds DMS through automated scripts or programs and (b) any attempts by non-dealer-employees to access the Reynolds DMS. Auth. P.I. Tr. 2-P [Auth. Dkt. 163] at 15, 16 (Testimony of R. Schaefer); Auth. Resp. to DSAF [Auth. Dkt. 145] ¶ 77; Declaration of S. Cottrell [Auth. Dkt. 51] ¶¶ 37-38; Ex. 20, REYMDL00015519 (2016 ERA Data Management Milestones).

RESPONSE: Disputed that Reynolds was targeting "threats." Reynolds's efforts to inhibit third-party access were, at least in part, driven by the profit motive of transitioning application vendors to RCI. *See* Response to Statement of Fact No. 11. Rather, Reynolds sought to impede legitimate dealer-authorized access. *See* Response to Statement of Fact No. 3. There is also no evidence that a data integrator has ever caused a security breach. *See* PJ SAF 16. Reynolds itself has conceded that it used Authenticom's services and would not have done so if it had any security concerns. *See* ACOM SUF 114-15. Moreover, there is no prohibition in Reynolds's

contracts with dealers against use of automated data polling by dealers or their agents. *See* Emmanual Ex. 5 [Dkt. 779-7] at -265 [redacted] Emmanual Ex. 6 [Dkt. 779-8] at -679 [redacted] (emphasis added). Disputed to the extent that Reynolds asserts the measures were access controls within the meaning of the Digital Millennium Copyright Act. *See* 17 U.S.C. § 1201(a)(3)(B). This is a legal conclusion to which no response is required. Further disputed that "automated" access or access by non-dealer employees were "threats." Reynolds cites no evidence to support that assertion.

20. One group that sought to access the Reynolds DMS through automated methods were the so-called "third-party integrators," or as Reynolds called them, "hostile integrators," "hackers," and "bandits." Ex. 3 at 314:12-315:4 (Brockman tr.); Ex. 37 at 28:12-18 (Hellyer tr.); Ex. 38 at 33:21-34:8 (Martin tr.); Ex. 16 at 217:5-15 (Lamb tr.); Ex. 23 at 19:18-20:25 (Reynolds 30(b)(6) Hall tr.).

RESPONSE: Undisputed that data integrators attempted to access Reynolds's DMS through automated means and that Reynolds called them "hostile integrators," "hackers," and "bandits." Disputed to the extent Reynolds asserts data integrators were "third parties" as opposed to "agents," which is a legal conclusion to which no response is required. Authenticom acted on behalf of dealers, which had the capability to control all aspects of Authenticom's data integration service. *See* ACOM SUF 26, 30, 33-44.

21. Authenticom was a third-party data broker throughout the relevant time period. Authenticom's business model with respect to the Reynolds DMS was predicated on using automated scripts to access the Reynolds DMS, utilize the DMS's internal features and functionality to display and report data, and exfiltrate that data back to Authenticom's servers. Authenticom referred to this process as "polling" a DMS. Authenticom would subsequently send that data on to third parties such as application vendors. *See generally* Ex. 33, AUTH_00141204 (Overview of R&R Polling); Declaration of S. Cottrell [Auth. Dkt. 51] ¶¶ 9, 25.

RESPONSE: Disputed that Authenticom was a "third-party data broker." Authenticom acted as dealers' agent for the purpose of providing data integration services. *See* ACOM SUF 26, 30, 33-44. Undisputed that Authenticom used automated programs to access the DMS in the same manner as a dealer employee and would extract data for use by application vendors that the dealer chose to use. *See id.* ¶ 27. Disputed to the extent Reynolds asserts this was Authenticom's sole service. Authenticom also provided write-back services and data standardization and cleansing. *See id.* ¶ 13; Fenske Ex. 109 [Dkt. 975-109] ¶¶ 3-11 (noting Authenticom "has also offered bi-directional data integration for more than a decade" and listing customers that have purchased write-back data integration services from Authenticom).

22. Authenticom also had available to it, and sometimes used, other methods to obtain data from the Reynolds DMS. Authenticom's primary alternative method involved having dealers export data themselves from the DMS (for example, using Reynolds's Dynamic Reporting application) and then transmit the exported data to Authenticom. Authenticom refers to this as "dealer FTP" or "dealer push." This method did not involve Authenticom or its automated processes directly accessing Reynolds's proprietary DMS. Declaration of R. Schaefer [Auth. Dkt.

97] ¶ 87; Ex. 24 at 70:10-19, 93:7-94:17 (Wiersgalla tr.); Ex. 44 at 141:12-142:21 (Hembd tr.); Ex. 96, AUTH_00150633.

RESPONSE: Undisputed that Authenticom could obtain data from Reynolds's DMS using "manual" push methods, including with Dynamic Reporting, and that these methods did not require Authenticom to access Reynolds's DMS software. Disputed to the extent that Reynolds claims these "manual" methods were adequate substitutes for automated data integration. "Manual" methods were more insecure, more inconvenient to a dealer, and more likely to lead to errors. *See* PJ SAF 30.

23. Authenticom contracted with various third parties that desired data residing in the Reynolds DMS, offering to extract that data for them in exchange for a fee. Typically, these extractions would occur on a daily basis via an automated "polling" process. However, Authenticom would often run its polling process multiple times each day on each DMS—with a separate polling process running for each different file type (sales data, service data, parts data, etc.). Ex. 28 at 118:16-22 (Clements tr.); Ex. 33, AUTH_00141204 (Overview of R&R Polling); Ex. 39 at 43:2-46:7 (Munns tr.).

RESPONSE: Undisputed that Authenticom charged application vendors a fee in exchange for its data integration services. Disputed that Authenticom's services were "[t]ypically" limited to daily extractions. The cited material refers to Authenticom's current services, which have been limited by Defendants' blocking efforts. *See* Wilkinson Ex. 28 [Dkt. 779-30] Clements Tr. 118:16-22. Disputed to the extent Reynolds asserts that Authenticom only had the capability of polling on a daily basis (or several times per day). Authenticom is capable of providing near real-time and writeback services. *See* Fenske Ex. 109 [Dkt. 975-109] ¶¶ 3-11, 16 (noting Authenticom "has

also offered bi-directional data integration for more than a decade" and listing customers that have purchased write-back data integration services from Authenticom).

24. To accomplish this, Authenticom would reach out to the dealer that had licensed the Reynolds DMS in question and ask them to provide one or more sets of DMS user credentials. [redacted] Ex. 28 at 151:10-152:13 (Clements tr.); Ex. 39 at 25:17-26:7, 247:14-248:15 (Munns tr.); Ex. 40 at 49:14-50:6 (Auth. 30(b)(6) Brown tr.); Ex. 41, AUTH_00431252; Ex. 42, AUTH_00431361; Ex. 43, AUTH_00170533; Auth. P.I. Tr. 1-A [Auth. Dkt. 164] at 108:4-19 (Testimony of S. Cottrell).

RESPONSE: Undisputed that Authenticom obtained DMS user credentials from dealers that had the right under their license agreement to authorize agents to use the Reynolds DMS. *See* Response to Statement of Fact No. 3. [redacted] *See* Dorris Ex. 154 [Dkt. 977-156] Shostack Rep. ¶¶ 52-53 & n.27.

25. Authenticom's automated polling software would use these credentials to log into the Reynolds DMS, utilize the DMS's functionality to run reports and process data, and then extract that data to Authenticom's servers—whereon much of that data was further processed and passed along to other third parties for a fee. Ex. 39 at 43:19-44:7, 52:1-55:6 (Munns tr.); Ex. 33, AUTH_00141204 (Overview of R&R Polling); Ex. 2 at 62:7-63:7, 290:8-291:23 (Kirby tr.).

RESPONSE: Undisputed.

26. Authenticom's automated polling process relied upon running unlicensed copies of Reynolds's software on Authenticom's own polling servers. That software included at least two programs for every poll: (i) either ERAccess or ERA Ignite, depending on which version a given dealer was using; and (ii) a copy of Reynolds' Software Manager application, which is intended to ensure that the dealer is using the correct software version and install updates as needed. Ex. 39 at 113:17-115:18 (Munns tr.); Ex. 2 at 161:11-162:23 (Kirby tr.); Ex. 28 at 146:14-147:15 (Clements tr.); Ex. 34, AUTH_00093108 (stating that Authenticom was running 21 copies of the 9/4/13 version of ERAccess and 397 copies of the 9/23/13 version of ERAccess and discussing the need to add more); Ex. 33, AUTH_00141204 (Overview of R&R Polling).

RESPONSE: [redacted] *See* Wilkinson Ex. 28 [Dkt. 779-30] Clements Tr. 147:16-19. Disputed that Authenticom's use of either ERAccess or ERA Ignite was unlicensed, which is a legal conclusion, to which no response is required. Authenticom's use of the DMS was authorized by dealers, who had the right to authorize Authenticom's use pursuant to their contracts with Reynolds. *See* Response to Statement of Fact No. 3; Wilkinson Ex. 2 [Dkt. 779-4] Kirby Tr. 161:11-162:2 (referencing "[t]he software the dealer authorized us to use to collect the data on their behalf"), *id.* at 165:12-13 ("I would say the usage of the software license is from the dealership, licensed by the dealership."); Wilkinson Ex. 28 [Dkt. 779-30] Clements Tr. 99:25-100:4 ("On behalf of the dealer we get it the same way they do, through their authorization of their user name and password and using their portal to do it since we are an agent to do that on their behalf."); Dorris Ex. 5 [Dkt. 977-6] Cottrell Decl. ¶ 24 ("Before Authenticom pulls data from a dealership, it gets specific authorization from the dealer.").

27. Authenticom admits that it [redacted] without a license agreement from Reynolds. Authenticom claims that it o[redacted] although Authenticom witnesses were unwilling or unable to identify any such dealer. Ex. 39 at 38:15-39:2 (Munns tr.); Ex. 2 at 161:11-166:25 (Kirby tr.); Ex. 44 at 120:22-121:16 (Hembd tr.); Ex. 28 at 99:22-103:16 (Clements tr.); Ex. 40 at 200:11-203:8 (Auth. 30(b)(6) Brown tr.).

RESPONSE: Disputed that Authenticom [redacted] without a license agreement from Reynolds. Reynolds's license agreement with dealers authorized Authenticom to use the Reynolds DMS. *See* Response to Statement of Fact No. 3. Further disputed that Authenticom witnesses were "unwilling" to state how Authenticom [redacted]. They either testified they did not know the answer or that they [redacted]. *See* Wilkinson Ex. 2 [Dkt. 779-4] Kirby Tr. 161:11-162:2 [redacted], *id.* at 165:12-13 [redacted] Wilkinson Ex. 28 [Dkt. 779-30] Clements Tr. 99:25-100:4 [redacted] Dorris Ex. 5 [Dkt. 977-6] Cottrell Decl. ¶ 24 ("Before Authenticom pulls data from a dealership, it gets specific authorization from the dealer.").

28. [redacted]

[redacted]. Ex. 33, AUTH_00141204 (Overview of R&R Polling); Ex. 2 at 47:24-49:19 (Kirby tr.); Ex. 40 at 137:8-140:9, 142:10-143:1 (Auth. 30(b)(6) Brown tr.).

RESPONSE: [redacted]. Authenticom used Reynolds's DMS software in the same manner as a dealer employee. *See* ACOM SUF 27.

29. As Reynolds introduced various controls to prevent automated third parties from accessing it DMS, Authenticom worked to circumvent or create workarounds for each of those measures in turn. Auth. P.I. Tr. 1-P [Auth. Dkt. 162] at 44:10-14 (Testimony of S. Cottrell) (admitting that from 2010 to 2017, Reynolds had been "actively blocking" Authenticom and Authenticom "does what it can to get around those blocks"); Authenticom Mot. for P.I. at 8 [Auth. Dkt. 61] (stating that Authenticom worked to "develop workaround solutions that circumvented Reynolds's efforts to block access"); Auth. 7th Cir. Resp. Br. at 12 ("Reynolds' efforts, however, were not entirely successful; Authenticom, CDK, and other integrators worked with dealers to develop workarounds."); Ex. 26, AUTH_468320 (chart of Authenticom responses to Reynolds's access controls over time).

RESPONSE: Disputed to the extent that Reynolds asserts Authenticom "circumvented" any measure within the meaning of the Digital Millennium Copyright Act. *See* 17 U.S.C. § 1201(a)(3)(A). This is a legal conclusion to which no response is required. Authenticom made efforts to maintain its lawful, dealer-authorized access. *See* Responses to Statement of Fact Nos. 3 and 11.

30. As set forth above, Reynolds implemented CAPTCHA prompts and challenge questions to prevent automated processes from accessing its DMS beginning in 2009. Authenticom developed various ways for its automated polling programs to get around Reynolds's CAPTCHA prompts. Ex. 45 at 75:6-80:11 (Robinson tr.); Ex. 28 at 31:16-32:17 (Clements tr.); Ex. 26, AUTH_468320.

RESPONSE: Authenticom incorporates its Responses to Statement of Fact Nos. 13 and 14. Disputed that Authenticom "got around" Reynolds's CAPTCHA. Authenticom responded to the CAPTCHA by providing the correct response. *See* ACOM SUF 91-98.

31. First, Authenticom developed a program called "Auto CAPTCHA," sometimes also referred to as the "memory reader." This method was purely programmatic—i.e., it relied on no human input at any point. This tool worked by "ripping open" program memory to find the CAPTCHA answer, then feeding it back into the prompt. Ex. 39 at 140:4-5, 148:11-149:19 (Munns tr.); Ex. 29 at 268:12-22 (Cottrell 2019 tr.); Ex. 45 at 77:5-10, 80:9-11 (Robinson tr.); Ex. 46, AUTH_00096097; Ex. 47, AUTH_00091915.

RESPONSE: Undisputed that Authenticom developed a program called Auto CAPTCHA to read the CAPTCHA answer and to respond to CAPTCHA prompts with that answer. Authenticom disputes Reynolds's characterization of this program's functioning. Authenticom used a "trivially easy" process of simply reading the answer from otherwise accessible memory on the computer. *See* Ho Ex. 58, Miracle Tr. 252:6-257:3.

32. Authenticom's own documents admit that using Auto-CAPTCHA was doing things "the 'wrong' way," and witnesses admitted that using it made them uncomfortable. Ex. 48, AUTH_00095693; Ex. 39 at 152:3-7 (Munns tr.). But as of February 26, 2014, Authenticom was still polling over 40% of Reynolds dealers using Auto-CAPTCHA. Ex. 49, AUTH_00083390.

RESPONSE: Disputed. Reynolds does not cite any document stating that Auto CAPTCHA was doing things the "wrong way." The reference to the "wrong way" in Wilkinson Ex. 48 [Dkt. 780-7] is to "answering captcha the 'wrong' way," meaning providing the incorrect answer. The author of the email, Bill Munns, was observing that he did not think providing an incorrect answer to the CAPTCHA would matter. Nor did Munns testify that Auto CAPTCHA made him "uncomfortable." He testified that he did not know whether there was anything "problematic" or "improper" about Auto CAPTCHA because he did not develop it. *See* Ho Ex. 13, Munns Tr. 146:1-10, 146:19-147:6, 148:1-8 ("Q. Do you think there's anything wrong with memory ripping to extract data from Reynolds' dealers? . . . A. I don't understand the process enough. I didn't build it. I wasn't involved in development. I just understood a high-level overview of what it was doing."). Munns testified that Steve Cottrell was not "too comfortable" with Auto CAPTCHA but did not know why. *Id.* at 152:3-14. Undisputed that Authenticom was using Auto CAPTCHA on behalf of 40 percent of Reynolds dealers as of February 26, 2014.

33. Authenticom also utilized CAPTCHA farms to answer Reynolds's CAPTCHA prompts. Authenticom's data extraction software would grab an image of the Reynolds prompt and send it automatically to a third-party vendor in Eastern Europe. Authenticom's primary CAPTCHA farm vendor was "Death By CAPTCHA." That vendor would transmit a suggested

answer back to Authenticom, which would automatically insert it into the Reynolds prompt. Ex. 33, AUTH_00141204; Ex. 28 at 138:5-16 (Clements tr.).

RESPONSE: Authenticom disputes Reynolds's characterizations. Authenticom used a vendor from Eastern Europe that used human beings to provide answers to CAPTCHA prompts. *See* ACOM SUF 93-95; Wilkinson Ex. 28 [Dkt. 779-30], Clements Tr. 138:22-23 ("There's a person that answers the question, correct.").

34. Authenticom's documents indicate it purchased hundreds of thousands of CAPTCHA answers for use on Reynolds's system. Ex. 50, AUTH_00280874; Ex. 51, AUTH_00280909; Ex. 52, AUTH_00280913; Ex. 53, AUTH_00280915; Ex. 54, AUTH_00280937; Ex. 55, AUTH_00281398; Ex. 56, AUTH_00281333; Ex. 57, AUTH_00281303; Ex. 58, AUTH_00281301; Ex. 59, AUTH_00281253; Ex. 60, AUTH_00315748; Ex. 61, AUTH_00281205; Ex. 62, AUTH_00281015; Ex. 63, AUTH_00280991; Ex. 64, AUTH_00280958; Ex. 82, AUTH_00281367; Ex. 65 at 79:19-88:9 (Noth tr.).

RESPONSE: Undisputed.

35. Authenticom also used a text recognition tool, called Tesseract, to solve Reynolds CAPTCHA prompts. This tool was able to read the text in the prompt and supply it to Authenticom's software for input. Ex. 40 at 172:3-22 (Auth. 30(b)(6) Brown tr.).

RESPONSE: Undisputed.

36. Authenticom also compiled a database of previous Reynolds questions with corresponding answers; Authenticom's software would leverage that database to answer the questions automatically. Ex. 40 at 170:15-171:16, 172:3-22 (Auth. 30(b)(6) Brown tr.); Ex. 66, AUTH_00092449 (discussing Authenticom's auto-answer repository).

RESPONSE: Undisputed.

37. Authenticom also used a piece of software called "CAPTCHA Bot," which would "farm out" CAPTCHA prompts to temps or other employees for answering. Ex. 40 at 161:4-8 (Authenticom 30(b)(6) Brown tr.); Ex. 46, AUTH_00096097; Ex. 67, AUTH_00092111 (discussing employee CAPTCHA coverage).

RESPONSE: Undisputed.

38. Authenticom engaged in a long-running campaign to avoid having its IDs detected and disabled by Reynolds's security measures. Ex. 68, AUTH_00171450 (compiling list of criteria to avoid in 2013); Ex. 33, AUTH_00141204 (compiling list of criteria to avoid in 2015); Ex. 26, AUTH_00468320.

RESPONSE: Undisputed that Authenticom tried to change its software so that it did not become flagged by Reynolds Suspicious User ID monitoring. Disputed to the extent that Reynolds asserts Authenticom violated the Digital Millennium Copyright Act. *See* 17 U.S.C. § 1201(a). That is a legal conclusion for which no response is required.

39. Authenticom asked Reynolds dealers for DMS user IDs that would not indicate they were being used by an automated third party. As stated by one employee, "we should be

asking for usernames indicative of someone with a human pulse." Ex. 69, AUTH_00168020. Authenticom's goal was to avoid detection by Reynolds. Ex. 70, AUTH_00168116 ("Be sure that the user name is formatted in the same manner as their normal employee user names").

RESPONSE: Undisputed that Authenticom requested credentials indicative of use by a human. Disputed to the extent that Reynolds asserts Authenticom violated the Digital Millennium Copyright Act. *See* 17 U.S.C. § 1201(a). That is a legal conclusion for which no response is required.

40. As part of its automated polling program, Authenticom developed a script called "Menu walk." Functionally, menu walking entailed Authenticom's polling script logging onto the Reynolds DMS, navigating automatically through the DMS's menus and screens, and then logging off. Ex. 39 at 105:13-21 (Munns tr.); Ex. 32, AUTH00219452.

RESPONSE: Undisputed.

41. But menu walking was not typically used to extract data. Ex. 39 at 107:8-12 (Munns tr.). As described by Authenticom, menu walking was "[u]sed for R&R cases to mimic someone randomly accessing the DMS thru-out [sic] the day (to fool R&R into thinking actual person instead of us)." Ex. 71, AUTH_00465304. In other words, Authenticom crafted its menu walking scripts to mimic a human dealership user and avoid detection by Reynolds Suspicious User ID security protocols. That was its sole function and purpose. Ex. 72, AUTH_00230422, at 5 (describing menu walk as "entered in PCM as a file type used to avoid R&R automated access lockouts, should not be discussed externally"); Ex. 73, AUTH_00242735 ("But you are right about the 2012 lockouts. That is when we had to use Menu Walk to avoid the "Automated Access" error

which was similar to the Disabled Profile error."); Ex. 26, AUTH_00468320 (listing Menu walking as a response to Reynolds locking out profiles).

RESPONSE: Undisputed that certain Authenticom employees described Menu Walk in those terms. Disputed that this was the "sole function and purpose" and that Menu Walk was not "used to extract data." Menu Walk's purpose was to "maintain" the "log-on" from going to "inactive status" so that the software could continue to provide Authenticom's data integration service. Ho Ex. 13, Munns Tr. 105:22-106:14.

42. Authenticom's documents demonstrate that in some cases Authenticom ran its menu walk scripts on Reynolds's DMS four times a day. Ex. 34, AUTH_00093108.

RESPONSE: Disputed. The document cited by Reynolds contains four lines from a diagnostic log. *See* Wilkinson Ex. 34 [Dkt. 779-36] at -108. Those four lines are not separate instances of Menu Walk running at different times during the day. The time stamps for the diagnostic log all occur within 0.1 seconds: 10:06:20.650 a.m. to 10:06:20.696 a.m. *See id.*

43. In July 2013, Authenticom temporarily ceased using its menu walk scripts, due to concern that Reynolds was detecting them and disabling the associated IDs. Ex. 74, AUTH_00168432. Authenticom subsequently discussed using its menu walk scripts again in 2015. Ex. 75, AUTH_00101801. And there are documents from as late as 2016 indicating that Authenticom continued to utilize its menu walk script on Reynolds profiles. Ex. 76, AUTH_00154490 at 493.

RESPONSE: Disputed. Authenticom ceased using Menu Walk in July 2013. *See* Wilkinson Ex. 74 [Dkt. 782-25] (July 3, 2013: "[W]e will be disabling all menu walks at this

time."); Wilkinson Ex. 71 [Dkt. 782-22] at -310 ("***PLEASE NOTE** – per 7/3/13 email from Heidi, no longer using Menu Walk*"). Undisputed that Authenticom employees discussed using Menu Walk in 2015 but not before "test[ing]" a "theory" regarding its use. Wilkinson Ex. 75 [Dkt. 782-26]. Wilkinson Exhibit 76 does not indicate that Authenticom used Menu Walk in 2016. In a list of 350 dealers, there is a single dealer whose name inadvertently includes the words "Menu Walk." Wilkinson Ex. 76 [Dkt. 782-27] at -493.

44. Authenticom deleted reports and records off the DMS to try and prevent Reynolds from detecting its use of user IDs to access the system and extract data. Ex. 77, AUTH_00221025; Ex. 78, AUTH_00091792.

RESPONSE: Disputed. Prior to Reynolds's blocking efforts, Authenticom "normally" "create[d] a report, [ran] the report, and then delete[d] it." Wilkinson Ex. 77 [Dkt. 782-28] at -025. Authenticom did this because there were "limitations on the number of reports on the system," Wilkinson Ex. 78 [Dkt. 782-29] at -797, and if these were not deleted, the dealer could "run . . . out of reports they can have on the system," *id.* at -793.

45. Authenticom also modified its polling programs to avoid using input methods that would give away its status as an automated user. As stated by Authenticom employees, the goal of these modifications was to "trick ERAccess into thinking that it was a real user sending the answer." Ex. 36, AUTH_00167914.

RESPONSE: Undisputed that Authenticom modified its programs to use keyboard input methods that Authenticom believed would cause its accounts not to be disabled. *See* Wilkinson

Ex. 36 [Dkt. 779-38]; Wilkinson Ex. 33 [Dkt. 779-35] at -205. Undisputed that the quoted language appears in the cited document.

46. Authenticom eventually began using a special port to simulate a physical keyboard—a practice that Authenticom itself described as "low-level input spoofing." Ex. 33, AUTH_00141204.

RESPONSE: Disputed that Authenticom used a "special port." Authenticom used the "virtual servers' PS2 port," and a PS/2 port is a standard input port used by keyboards. *See* https://techterms.com/definition/ps2. Undisputed that the quoted language appears in the cited document.

47. Authenticom arrived at its keyboard spoofing solution after attempting various other methods to avoid detection. Ex. 36, AUTH_00167914; Ex. 79, AUTH_00170407; Ex. 35, AUTH_00141219; Ex. 68, AUTH_00171450.

RESPONSE: Undisputed that Authenticom tried several changes to its software to prevent its login credentials from being flagged for disabling. Disputed that "keyboard spoofing" was a "solution." The only "solution" to the disabling of Authenticom's login credentials was for Authenticom to request that the dealers provide new login credentials. *See* ACOM SUF 85. Indeed, the documents on which Reynolds relies shows that Authenticom tried changing the means by which it submitted input to the Reynolds DMS in May 2013, Wilkinson Ex. 36 [Dkt. 779-38], and October 2013, Wilkinson Ex. 79 [Dkt. 782-30], to no avail. Authenticom's login credentials continued to be disabled in November 2013, Wilkinson Ex. 68 [Dkt. 782-19], and May 2015, Wilkinson Ex. 35 [Dkt. 779-37].

48. Authenticom also worked to manipulate the serial numbers used by its polling servers in an effort to avoid detection. Over time Authenticom became concerned that its use of rotating serial numbers (within the Reynolds software on its polling servers) was causing its profiles to be disabled. Ex. 39 at 113:17-115:18 (Munns tr.); Ex. 80, AUTH_00094637 (email chain re "Disabled Profiles Caused By Serial Number Changes"); AUTH_00174085 ("We put the logic in place to prevent disablings on certain UserIDs tied to a serial."). Authenticom eventually sought to avoid that problem programmatically: "Each UserID is tied to a Serial# that is controlled by our polling launcher (PCM)." Ex. 33, AUTH00141204.

RESPONSE: Undisputed that Authenticom became concerned that its method of access – which generated multiple serial numbers for each dealer – might cause its credentials to be disabled. *See* Wilkinson Ex. 80 [Dkt. 782-31] at -637 ("[W]e generated 45 for one dealer in the last day. I have no solid idea why these are being generated on there."). Disputed that Authenticom "manipulate[d] the serial numbers." Authenticom assigned a specific login credential to each serial number. *See* Wilkinson Ex. 33 [Dkt. 779-35] at -204 ("Each UserID is tied to a Serial# that is controlled by our polling launcher (PCM)"). Disputed to the extent that Reynolds asserts its Suspicious User ID Monitoring program actually flagged accounts for disabling based on serial numbers – a fact for which Reynolds asserts no supporting evidence. Further disputed to the extent that Reynolds asserts that Authenticom assigning a specific login credential to each serial number had any effect on the disabling of Authenticom's login credentials. *See id.* (May 8, 2015: "How we handle Serial# management differs between Authenticom (by IP Address and UserID) and DealerVault (by DealerID), but lockouts in both environments tell me how we're particularly handling this either [is] not important or wrong altogether.").

49. Authenticom knew that its access to the Reynolds DMS was unauthorized by Reynolds. Reynolds had informed the world since at least 2007 that it did not approve of third parties accessing its DMS. Reynolds made repeated announcements to its customer base and the market that third-party access to its DMS was prohibited. Ex. 82 (February 19, 2007 Automotive News Article); Ex. 107, REYMDL00012341 (February 4, 2007 Automotive News Article) ("Reynolds, with about 11,000 dealership customers in the United States, has warned dealers that they are violating their contracts when they provide log-ins and passwords to third-party vendors."); Ex. 97, REYMDL00015601 (April 2007 Automotive News Article) (reporting that in 2006 "Reynolds and Reynolds Co. began informing dealers they would be violating their contract if they allowed third parties to access directly the Reynolds dealer management system"); Ex. 98, REYMDL01075600 (March 2012 Automotive News Article) ("What we're [Reynolds] trying to do is block unmonitored automated access to the DMS."); Ex. 18, REYMDL00022899 (Fuel Article January 1, 2010: "It remains our policy to not allow 'hostile interfaces' or unauthorized code on your systems to protect both Reynolds and your dealership from security breaches and potential data corruption issues."); Authenticom Compl. [Auth. Dkt. 1] ¶¶ 6, 92, 103, 106-107, 109, 185.

RESPONSE: Disputed. As explained above, Reynolds's license agreement with dealers gave dealers' agents the right to use the DMS. *See* Response to Statement of Fact No. 3. The premise that Authenticom's access was unauthorized by Reynolds is therefore inaccurate. Moreover, Authenticom employees testified that they believed they were properly authorized to access Reynolds's DMS as dealers' agents. *See* ACOM SUF 28. Undisputed that Reynolds has publicly claimed that third-party access to its DMS is prohibited, but Authenticom did not

understand this position to override (or have the ability to override) the terms of Reynolds's dealer contracts. *See id.*

50. Reynolds backed those announcements with concrete enforcement steps, and Authenticom was aware of Reynolds's policy and desire to prevent third parties from accessing its DMS without Reynolds's permission. Ex. 93, REYMDL00015727 (Authenticom receiving Reynolds's 2011 announcement that it was rolling out measures to prevent automated access to the Reynolds system); Ex. 26, AUTH_00468320 (chart of Reynolds measures and Authenticom responses); Ex. 83, AUTH_00472681 (Authenticom CEO noting in 2013 that Reynolds had been saying for 8 years that they were "going to lock everyone out"); Ex. 84, AUTH_00170766 (Authenticom COO suggesting to CEO in 2013 that when requesting new Reynolds IDs "we point out that RR is doing this because they don't want us polling the data").

RESPONSE: With respect to Reynolds's "concrete enforcement steps," Authenticom incorporates by reference its Responses to Statement of Fact Nos. 13-20. Undisputed that Authenticom was aware of Reynolds's desire to prevent third parties (but not agents) from accessing its DMS. Disputed that Reynolds had effectuated a policy to prevent third parties from accessing its DMS until approximately 2017. *See* Response to Statement of Fact No. 11. Authenticom believed it had the legal right to use the Reynolds DMS and it did not understand Reynolds's public disapproval of third-party access to override (or have the ability to override) the terms of Reynolds's dealer licenses. *See* Response to Statement of Fact No. 49.

51. Authenticom announced to its customer base in 2013 that Reynolds was "steadfast in their commitment to remove all 3rd party access points to their systems." Ex. 19, AUTH_00170940.

RESPONSE: Undisputed. However, to the extent Reynolds suggests that this statement indicates a subjective belief on the part of Authenticom that its use of the Reynolds DMS was unauthorized, that suggestion is disputed. *See* Responses to Statement of Fact Nos. 49-50.

52. Authenticom's executives admitted that they knew Reynolds objected to their accessing the Reynolds DMS. Ex. 29 at 21:11-12 (Cottrell 2019 tr.) ("Reynolds does not want us polling data from their systems"); Ex. 85 at 100:1-6; 128:14-16 (Gentry tr.) ("Q: And they [Reynolds] wanted Authenticom to stop accessing their DMS? A: Oh, hell yeah."); Ex. 28 at 60:5-63:22 (Clements tr.) (admitting that he had seen warnings in the Reynolds DMS in 2013 stating that third-party access was prohibited by the Reynolds license agreement); Ex. 86, AUTH_00091619, at 621.

RESPONSE: Undisputed that Authenticom employees testified as stated. Disputed to the extent Reynolds asserts Authenticom employees admitted a lack of authorization to access Reynolds's DMS. *See* Responses to Statement of Fact Nos. 49-50; Decl. Ex. 306 [Dkt. 979-106] Cottrell Tr. 21:10-13 ("I would agree with you that Reynolds does not want us polling data from their systems. I believe that is because they don't want to compete with us."); Wilkinson Ex. 85 [Dkt. 782-36] Gentry Tr. 128:13 ("A. They wanted the RCI business. It was printing money. Q. And they wanted Authenticom to stop accessing their DMS? A. Oh, hell yeah.").

53. Authenticom's CEO testified that Reynolds's view as to whether Authenticom's access to and use of Reynolds's DMS was improper "wasn't part of what the consideration was." Ex. 29 at 270:10-19 (Cottrell 2019 tr.).

RESPONSE: Disputed. Authenticom's CEO testified that "Reynolds's view . . . of whether [Authenticom] should be using automated responses to answer CAPTCHA . . . wasn't part of what the consideration was." Wilkinson Ex. 29 [Dkt. 779-31] at 270:10-19. As Authenticom's CEO explained: "Reynolds introduced CAPTCHA. Dealers had to answer CAPTCHA questions when we were provided usernames and passwords. They asked us to answer the CAPTCHA questions on their behalf as their agent." *Id.* at 172:13-21. Further, Authenticom did not understand Reynolds's public disapproval of its access to override (or have the ability to override) Authenticom's authorization to access Reynolds's DMS. *See* Responses to Statement of Fact Nos. 49-50.

54. The ERA DMS login screen—seen every time a user accesses the system—further announced Reynolds's prohibition on any copying, accessing, or use of the system by any third party. Authenticom employees admitted seeing and being aware of this notification. Ex. 87, AUTH_00175368; Ex. 88, AUTH_00472396; Ex. 89, AUTH_00155147, at 151; Ex. 39 at 351:13-356:19 (Munns tr.); Ex. 2 at 174:22-179:4 (Kirby tr.); Ex. 44 at 121:18-128:20 (Hembd tr.).

RESPONSE: Undisputed that the ERA DMS contains a login screen shown every time a user accesses the system that states the software cannot be "shared with or accessed by a third party electronically or manually," although the login screen does not mention a dealers' agents. *See* Wilkinson Ex. 87 [Dkt. 782-38] at -368; Wilkinson Ex. 88 [Dkt. 782-39] at -396; Wilkinson Ex. 89[(Dkt. 782-40] at -151. Undisputed that certain Authenticom employees were aware of this

login screen. However, Authenticom's employees testified that they did not understand Reynolds's public disapproval of third-party access to override (or have the ability to override) Authenticom's authorization to access the Reynolds DMS. *See* Responses to Statement of Fact Nos. 49-50.

55. Reynolds also sent Authenticom an express cease-and-desist letter in 2015, demanding that it cease accessing the Reynolds DMS. Ex. 91, REYMDL00012553.

RESPONSE: Undisputed.

56. Reynolds provided the court's ruling in the *SIS* case to Authenticom, along with the contractual language it was based upon. Ex. 90, AUTH_00468019.

RESPONSE: Undisputed that Reynolds's sent a ruling from the *SIS* case to Authenticom. Further undisputed that Reynolds sent Authenticom contractual language that Reynolds relied upon. Disputed to the extent that Reynolds asserts it sent Authenticom all relevant contractual language. Reynolds supplied Authenticom with heavily redacted contracts. *See* Wilkinson Ex. 90 [Dkt. 782-41] at -038 to -048. These contracts omitted the relevant language that dealers' [redacted]. Emmanual Ex. 6 [Dkt. 779-8] at -679; Emmanual Ex. 4 [Dkt. 779-6] at -044.

CONCLUSION

Reynolds's motion for summary judgment should be denied.

Dated: July 28, 2020

Respectfully submitted,

/s/ Derek T. Ho

Derek T. Ho
KELLOGG, HANSEN, TODD, FIGEL & FREDERICK, P.L.L.C.
1615 M Street, NW, Suite 400
Washington, D.C. 20036
(202) 326-7900
dho@kellogghansen.com

Counsel for Plaintiff Authenticom, Inc.

CERTIFICATE OF SERVICE

I, Derek T. Ho, an attorney, hereby certify that on July 28, 2020 I caused a true and correct copy of the foregoing **PLAINTIFF AUTHENTICOM, INC.'S RESPONSES TO COUNTERCLAIMANT'S THE REYNOLDS AND REYNOLDS COMPANY'S STATEMENT OF UNDISPUTED MATERIAL FACTS IN SUPPORT OF ITS MOTION FOR PARTIAL SUMMARY JUDGMENT** to be filed and served electronically via the court's CM/ECF system. Notice of this filing will be sent by e-mail to all parties by operation of the court's electronic filing system or by mail to anyone unable to accept electronic filing as indicated on the Notice of Electronic Filing. Parties may access this filing through the court's CM/ECF system. Copies of the Under Seal filing were served on counsel of record via email.

/s/ Derek T. Ho

Derek T. Ho
KELLOGG, HANSEN, TODD, FIGEL & FREDERICK, P.L.L.C.
1615 M Street, NW, Suite 400
Washington, D.C. 20036
(202) 326-7900
dho@kellogghansen.com